DSCP-DOD-Medical Device Vendor Industrial Conference

Information Assurance Vulnerability Alerts (IAVA)

Air Force Medical Support Agency (AFMSA)
Clinical Engineering Branch
Fort Detrick Maryland

29 September 2004

Goals

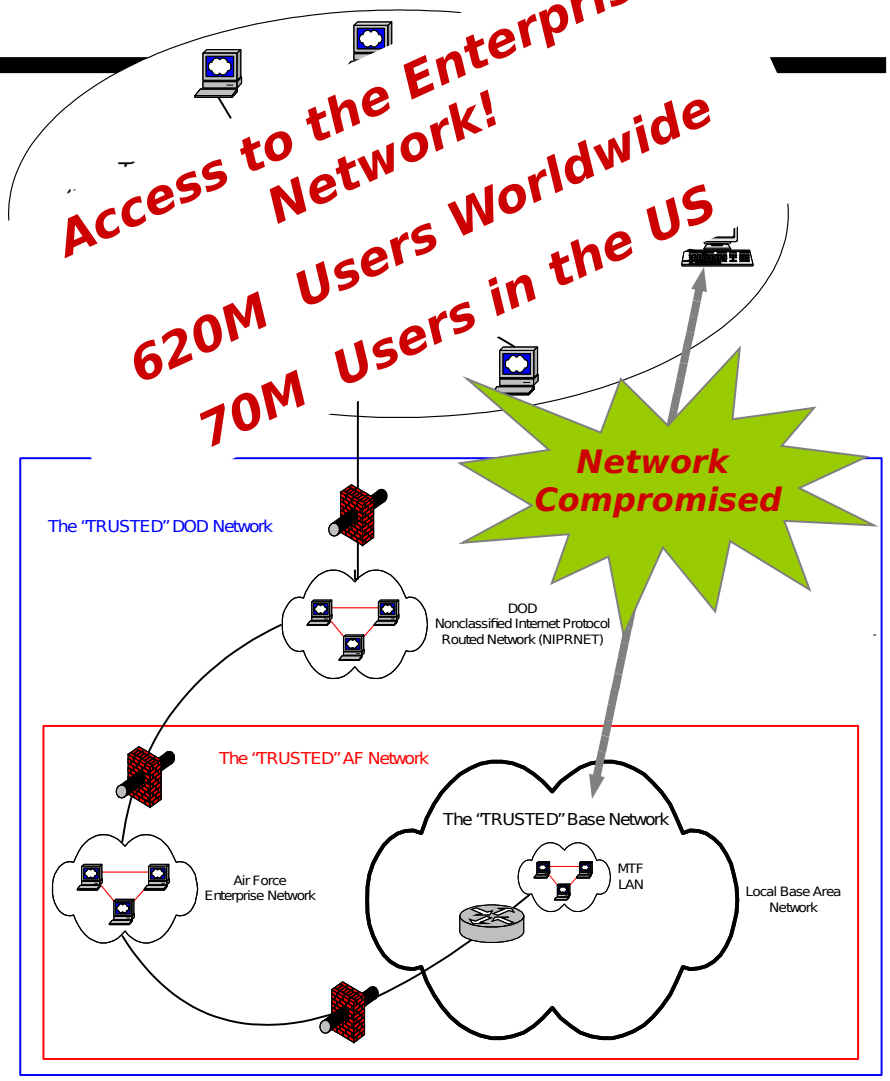
- **Clarity**
  - ✓ What is an IAVA?
  - ✓ Why Should I Care?
  - ✓ Why is it My Problem?
  - ✓ The Marketplace
- **Collaboration**
  - ✓ Team Approach
  - ✓ Centralized Mechanisms
  - ✓ References

IAVA – What?

- **Information Assurance Vulnerability Alert**
  - ✓ Originates from Carnegie Mellon
    - Computer Emergency Response Team (CERT)
    - Response to Known Bugs, Hacks, and Attacks
    - Alerts Distributed via CERT List Server
  - ✓ DOD-CERT
    - DOD-CERT Team Response to CERT
    - Assess Vulnerability from DOD Perspective
      - Often Alters Response and Milestones
      - Distributed via DOD-CERT list Server (.mil restricted)
  - ✓ Service Specific Alerts and Bulletins

Who Are the Stakeholders? IAVA – What's the Issue?

- ✓DoD & VA
  - •All Branches
  - •All VISNs
- ✓Medical Device Vendors
  - •All Device Manufacturers
  - •All Networked Devices
- ✓Our Customers
  - •Healthcare Providers
  - •Healthcare Consumers


Access to the Enterprise Network!
620M Users Worldwide
70M Users in the US
Network Compromised
The "TRUSTED" DOD Network
DOD Nonclassified Internet Protocol Routed Network (NIPRNET)
The "TRUSTED" AF Network
The "TRUSTED" Base Network
Air Force Enterprise Network
MTF LAN
Local Base Area Network

The Marketplace

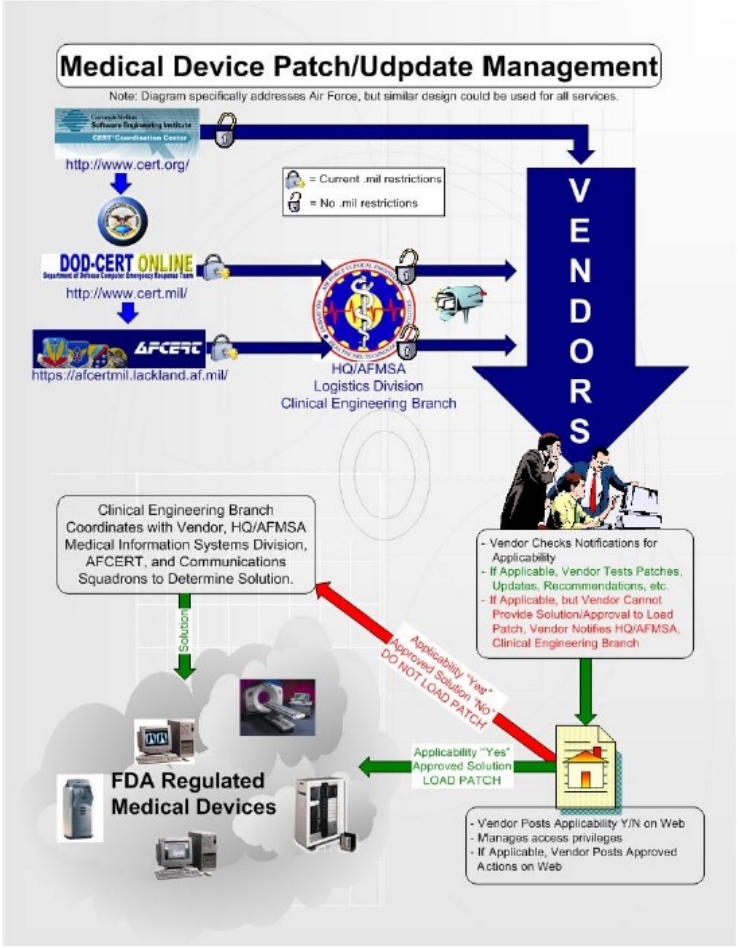
- **FDA and the 510(k)**
  - ✓ Good Manufacturing Practices (GMP)
  - ✓ Software Validation
  - ✓ Design Security in at Product Development
- **HIPAA**
  - ✓ Due Care vs. Due Diligence
  - ✓ Reasonable Measures to Protect PHI
- **Service Maintenance Agreements**
  - ✓ Cost of Doing Business
  - ✓ Required to Meet Federal Mandates

Collaboration

- **Team Approach Required**
  - ✓ Medical Device Vendor Processes
  - ✓ DOD/Services Processes
  - ✓ Project Management Oversight
  - ✓ End-User Implementation
- **Centralized Mechanisms**
  - ✓ Information Flow:
    - CERT Notification
    - Patch Validation
    - Patch Reporting, Processing, and Installation
  - ✓ Close the Loop – Secure the Device

Collaboration

- **Reference Model:**
  - ✓CERT – Proactive
  - ✓Service-Centric
  - ✓Web-Based Interface
  - ✓Secure Access
    - Platforms Impacted
    - Validation Status
    - Validation ECD
    - Installation
- **Long-Term:**
  - ✓Single-Point Updates
  - ✓Remove Middle-Man


Medical Device Patch/Udpdate Management
Note: Diagram specifically addresses Air Force, but similar design could be used for all services.
http://www.cert.org/
= Current .mil restrictions
= No .mil restrictions
VENDORS
DOD-CERT ONLINE
http://www.cert.mil/
AFCERT
https://afcertmil.lackland.af.mil/
HQ/AFMSA
Logistics Division
Clinical Engineering Branch
Clinical Engineering Branch Coordinates with Vendor, HQ/AFMSA Medical Information Systems Division, AFCERT, and Communications Squadrons to Determine Solution.
- Vendor Checks Notifications for Applicability
- If Applicable, Vendor Tests Patches, Updates, Recommendations, etc.
- If Applicable, but Vendor Cannot Provide Solution/Approval to Load Patch, Vendor Notifies HQ/AFMSA, Clinical Engineering Branch
Solution
Applicability "Yes" Approved Solution "No" DO NOT LOAD PATCH
Applicability "Yes" Approved Solution LOAD PATCH
FDA Regulated Medical Devices
- Vendor Posts Applicability Y/N on Web
- Manages access privileges
- If Applicable, Vendor Posts Approved Actions on Web

IA Vulnerability Alerts

- **Clarity**
  - ✓ What is an IAVA?
  - ✓ Why Should I Care?
  - ✓ Why is it My Problem?
  - ✓ The Marketplace
- **Collaboration**
  - ✓ Team Approach
  - ✓ Centralized Mechanisms
  - ✓ References
- **Questions**

IA Support References

- **Vulnerability Alerts:**
  - ✓ CERT Coordination Center
    - http://www.cert.org
  - ✓ CERT Advisories Mailing List
    - http://www.cert.org/contact_cert/certmaillist.html

- **Configuration Guidelines:**
  - ✓ Defense Information Systems Agency (DISA) – Information Assurance Support Environment
    - http://iase.disa.mil/policy.html (Public Site)
  - ✓ National Security Agency (NSA)
    - http://www.nsa.gov/

- **Security Related Resources:**
  - ✓ National Institute of Science and Technology (NIST) – Computer Security Resource Center (CSRC)
    - http://csrc.nist.gov/publications/nistpubs/index.html
  - ✓ National Information Assurance Certification and Accreditation Process (NIACAP)
    - http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf
  - ✓ Common Vulnerabilities and Exposures
    - http://cve.mitre.org/
  - ✓ Computer Security Institute
    - http://www.gocsi.com/
  - ✓ Center for Internet Security
    - http://www.cisecurity.org/